# Smart Card and its Application in Software Protection

William Xie
wxie007@ec.auckland.ac.nz
Department of Computer Science
The University of Auckland
Lecturers: Prof Clark Thomborson, Prof Jim Goodman

**Abstract**

*Smart card is a small and powerful security tool, which can support variety of applications. Software protection against software piracy is an important issue in the field of computer security. This paper overviewed the smart card technology, and then explained two different schemes with smart card. These tow schemes can be applied in different situations.*

**Key words:** smart card, software protection, one-time install solution, asymmetric cryptosystem

## § 1 Introduction

Software piracy has become important security problem since computer became popular. Unlike other products, software is easier to be copied. The cost is very cheap compared with creating the software. Although most of countries have the software copyright law to prevent piracy, the effect is not ideal as people expect. Software piracy likes two-blade sword: it reduce the profits of the software producer and pirate copies are partially paid by the legal users. At the other side, it will make the software producer no passion create more new software. From the perspective of the country, the trade of the software will not develop effectively.

Today most software products have weak protection: usually check something like username, password and serial no when installation. However, it is vulnerable to some software analyze tools like “soft-ice” or technical of reverse engineering. The

popularity of Internet made it more convenient to get this information because some dishonest users published the authentic passwords or serial no in some websites.

To prevent these software piracy attacks, people have two different methods: software technology and hardware technology. Some times people believe the pure software technology can solve this problem. The common technical is: serial-no mode, key-file, limited time, watermarking, and code obfuscation. Other methods, like extracting some hardware devices information to produce the registration number by some specially algorithm, need to check the number when installation. This mechanism is inconvenient when the users update their hardware. All of those methods mentioned above had not achieved satisfied effect. Theoretic approaches have demonstrated that a solution completely based on software is unfeasible. [4]

The hardware components are difficult to duplicate, this feature makes people more interested in various hardware protection approaches. The protected software always checks the presence of the hardware and communicates with hardware when the software runs. Hardware keys and dongles are the typical application for this method. But it is also vulnerable to some special tools and has the compatibility problem with different operation system.

Smart cards, especially those with processor-enabled smart cards, are often used in applications, which require strong security protection and authentication. This paper will focus on the software protection application. In section 2, we will depict the overview of smart cards proposed by Katherine. [3] Section 3 will analyze the software protection scheme proposed by Mana. [1] Section 4 will present another solution proposed by Chu-Hsing Lin. [2], Comparison with those two methods is presented in section 5 and section 6 summarizes the conclusions.

## § 2 Smart Card Overview

In this section, we will introduce the history, type and standard of smart cards, and then the typical application will be presented as well as the comments on [3].

## §2.1 Smart Card History

Two German inventors patented the idea of having plastic cards in 1968. The following table 1 presents a brief outline of the evolution of the smart card. [3]

| Year | Event |
|---|---|
| 1968 | 2 German inventors patent combining plastic cards with micro chips |
| 1970 | Arimura invents and patents in Japan |
| 1974 | Roland Moreno invents and patents in France |
| 1976 | French DGT initiative, Bull (France) first licenses |
| 1980 | First trials in 3 French cities |
| 1982 | First U.S. trials in North Dakota and New Jersey |
| 1996 | First university campus deployment of chip cards |

**Table 1.** Outline of the evolution of the smart card

France was an early smart card proponent and now smart cards were widely used in German and France, mainly used in healthcare and financial system. Their investments proved profitable. It not only dropped credit card fraud rates but also facilitate patient to get better treatment. For concerns about security, the U.S. government plans to issue millions of smart cards.

## §2.2 Smart Card Type and Standards

There are tow type of smart cards: memory card and processing-enabled card. The main difference between them can be described as Table 2. [3]

| Feature Component | Memory Card | Processor-Enable Card |
|---|---|---|
| Random Access Memory? | no | yes |
| Microprocessor? | no | yes |
| Data flow | One-dirctional | Bi-directional |

| | | |
|---|---|---|
| Data certified secure | no | yes |
| Available memory | 8bytes to 2KB | 64KB to 1MB |
| Cost | cheap | expensive |
| Example | Phone card | Multi-application cards |

**Table 2.** Memory versus process-enabled smart cards

The typical architecture of processor-enabled smart card module is shown in Figure 1.

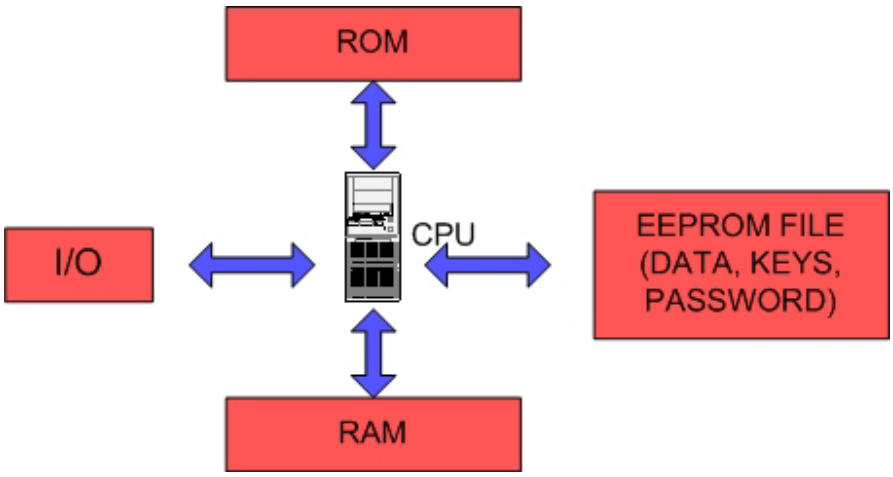



**Figure 1.** Architecture of a smart card

Such cards have an embedded silicon-based processor, and ia almost as powerful as the desktop PCs of the early 1980s.

The Switzerland-based International Organization for Standardization defines several standards: ISO 7816-1, ISO 7816-2, ISO 7816-3, ISO 7816-4 and ISO7816-7, described physical character, size, electrical contacts, electrical signals and transmission protocol and query language commands for the standard smart card.

### §2.3 Use for Smart Card

The smart card mainly used in authentication, authorization and transaction processing.

Smart cards can authenticate the users' personal identifications base on the users' passport or users' PIN number. Therefore, it can be applied in drivers' licenses to contain driving records and other information.

Smart cards also can offer data encryption for the cardholder. In the healthcare system, smart cards could help "automate and standardize patient demographic information on medical records" [3] as well as facilitate drug prescription fulfillment.

Web-based or traditional trade transaction also benefit from smart cards because it supply more secure function through data encryption. GSM, voting and other commerce are tending to use smart cards to preventing all kinds of fraud.

## §2.4 Comments on [3]

Katherine gave us the basic knowledge about smart cards; it is good to those who have never heard about the smart card technology. The main defects for this article lie in two points. Firstly, it did not give us any idea how to apply it for the requirement of security. Secondly, the threat of smart card had not been presented.

From this article, we can infer the security application can be depicted as Figure 2.

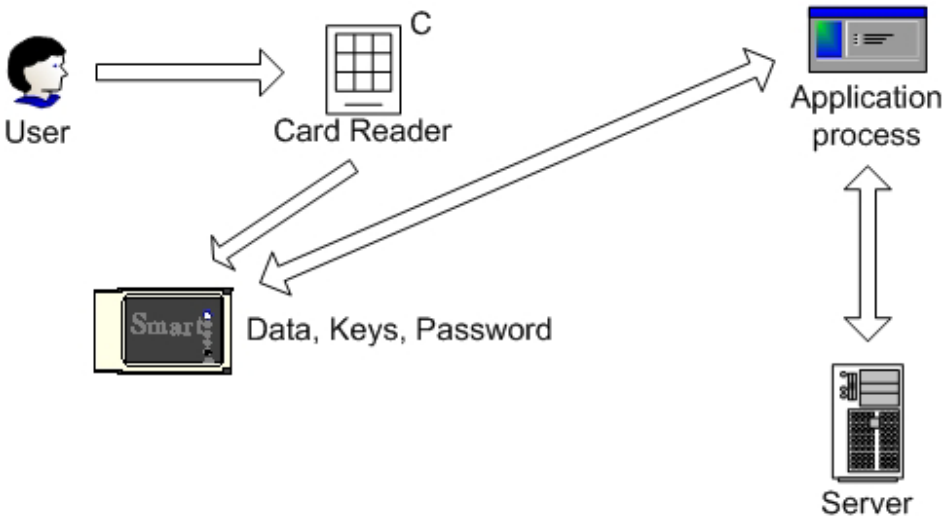



**Figure 2.** Example of application

First, the user inserts his card to the card reader, input password or biometric identification so that the card can verify the legal user. The card can have the function of lock down after a pre-determined number of incorrect passwords have been entered. Then the smart card and application process will verify each other. After that, the transaction begins with all data being encrypted.

## § 3 Software Protection Scheme 1

Mana presented a robust software protection scheme based in the use of smart cards and cryptographic techniques. He introduced tow new schemes, (The second one is more efficient than the first one.) suggest how to manage the license: sale, transfer and recovery. He also discussed all kind of possible attack on his new schemes and how to prevent these attacks. We will analyze his final efficient scheme in detail and discuss the advantage and disadvantage of this scheme.

### § 3.1 Mana's Scheme

Mana's robust and efficient scheme is shown in Figure 3.

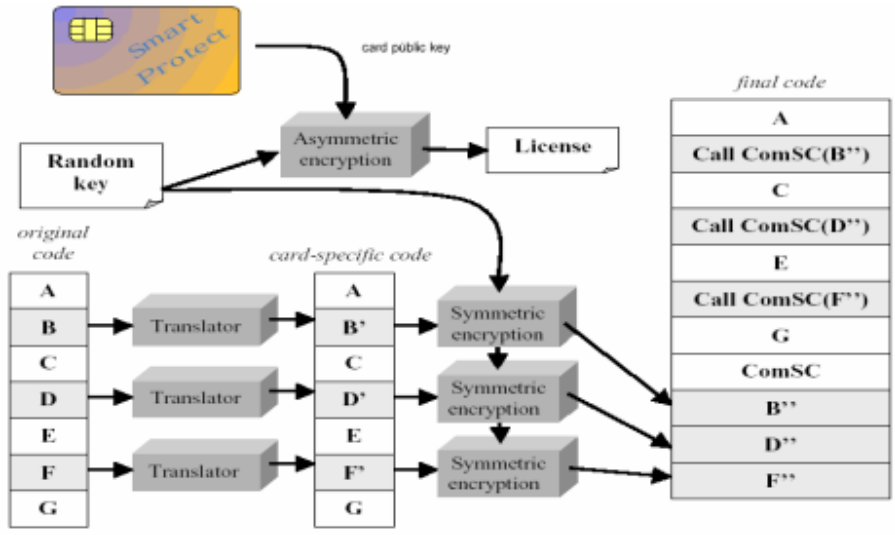



**Figure 3**. Mana's efficient scheme

The scheme can be divided into two phases: production phase and authorization phase. In the production phase, the software vendor will choose the protection section in the original code, including code and data. For example, in the Figure 3, it is B, D and F. Then they use the translator to change the original code to card-specific code. For instance, if the card is JVM, the B' can be java class file. After that, the vendor will pick up a random key depending on the individual client information, e.g., the client name or telephone no. Finally the protected section will be encrypted using the random key with a symmetric cryptosystem and the encrypted section will be kept in the smart card.

In the authorization phase, firstly, the random key, information about conditions of use, the identification of the software and license, were encrypted with a symmetric cryptosystem, i.e., all this information is encrypted with the card public key and kept in the card. The public key can be extracted by the card reader while the private key never be transmitted outside the card.

The client will get the software as well as the smart card. When he installs the software, the card will verify the license. If the verification is success, the random key will be decrypted. As the final code call the encrypted protected section B'', the smart card will use random key to decrypt B' and execute it inside of the card. After that, the smart card will return the result to the call function.

### § 3.2 Comments on Scheme 1

The principle of this scheme something likes the encryption method PGP that has the better balance between security and speed. The Asymmetric encryption is secure and only the license needs to be encrypted in this method. The large number of code and data can be encrypted and decrypted with symmetric encryption in the rapid speed.

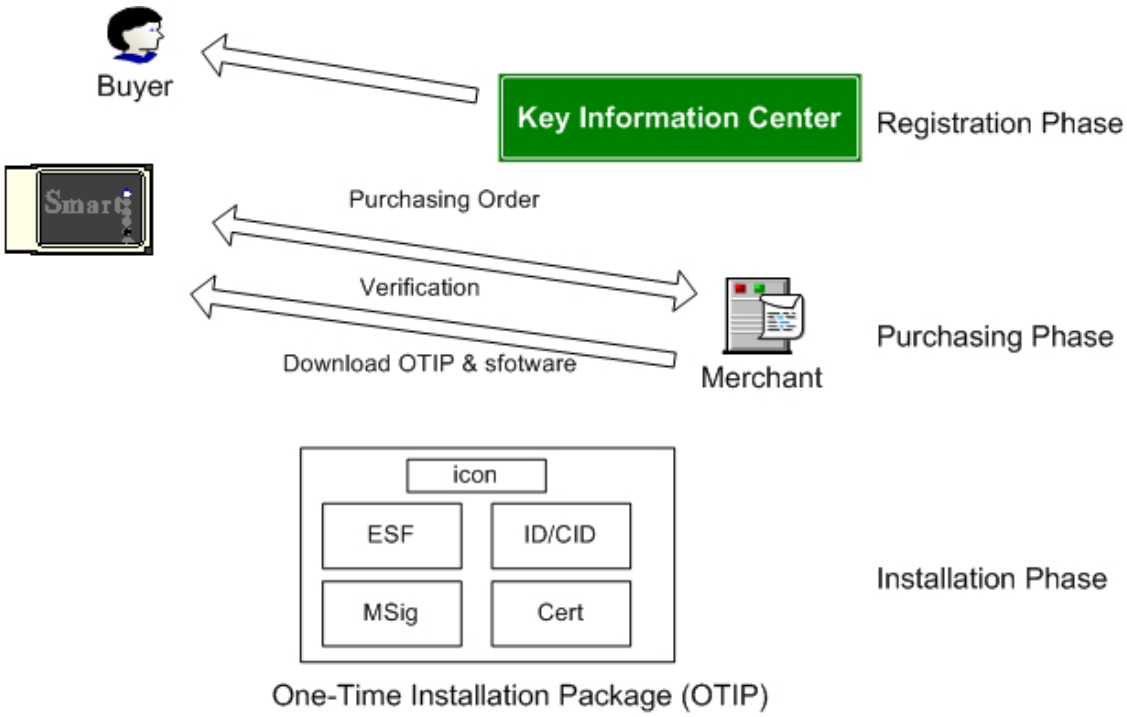
The main defect of this scheme is that we must use database to manage clients' license, so the database will have a great number of transaction for verification. It is not feasible to those widely used software products.

## § 4 Software protection Scheme 2

Chu-Hsing Lin and Chen-yu Lee proposed an innovative software protection scheme, which the client can purchase software from the Internet using his (or her) smart cards. But the software can only be installed one time.

### § 4.1 Lin and Lee's Scheme

Their scheme can be shown in Figure 4.




**Figurer 4**. Lin and Lee's innovative scheme

Their scheme is divided into three phase: registration phase, purchasing phase and installation phase.

In the registration phase, they assume there exists a trusted key information center (KIC) that is responsible for managing and issuing smart cards to user. If one client applies for a smart card from KIC, he will get a card with identity, password, private and public key, and a certification.

In the purchasing phase, when the client send the purchasing order to the software

producer's server by smart card, the server will verify the certification and signature. If passed check, the server will produce the OTIP, which include encrypted original setup file, client's ID, card number CID, signature Msig and merchant's certificate Cert.

In the installation phase, after the client get the OTIP and execute it. During execution, the client is requested to insert the smart card for verification. The smart card will send the its parameter to OTIP, OTIP then decrypt the original setup file and install the software.

During the process, they extract the client-computer's timestamp and OTIP will stop execute if timestamp is incorrect.

### § 4.1 Comments on Lin and Lee's Scheme

Their scheme not only has the rigid verification during the purchasing phase and installation phase, but also it can trace the traitor for illegal copy and transfer.

However, as they discussed in the article, this scheme request the original setup file have the ability to resist the duplication. This defect lies in the original setup file does not communicate with the OTIP.

This scheme can only be applied in buying software from the Internet, and it also request the software producer have a powerful database to deal with the verification. These limit the application of this scheme.

## § 5 Comparsion

The similarities of these tow schemes lie in: Firstly, both of them require the smart card has the computation, verification function, so this type of smart card is belong to processor-based card; Secondly, both of them use the asymmetric cryptosystem to encrypt the small amount of key information; Thirdly, both of them request the software producer have server to verify the smart card; Finally, both of them had the good balance between security and speed.

The difference of these two schemes is also obviously: Firstly. The smart card can execute the card-specific code in scheme 1 while it need not have this function in scheme

2; Secondly, the software must call the result of the protection section in smart card in scheme1, but the software of scheme 2 will not call any data in the smart card; Thirdly, per application need one smart card in scheme 1 while one smart card can be used in multi-application in scheme 2; Finally, scheme 1 can not be applied in the Internet because the cards must be distributed with the software, on the contrary, scheme 2 must be applied in the Internet.

## § 6 Conclusion

Smart card is a powerful security tool with the development of the computer technology. Although there is a lot of difficult to use it widely, e.g., the cost problem, the standard problem, we believe it will be spread through the world like personal computer. Using the smart card to protect the software is interesting topic in the fields of information security since there are no completely secure solutions. These two software protection scheme we had mentioned also had their vulnerability, however, as the Mana said “the objective of a software protection scheme is to make the attack to the scheme difficult enough to discourage dishonest users”.

## Bibliography

[1] Antonio Mana, Ernesto Pimentel, *An Efficient Software Protection Scheme,* in Michel Dupuy, Pierre Paradinas (Eds.): Trusted Information: The New Decade Challenge, IFIP TC11 Sixteenth Annual Working Conference on Information Security (IFIP/Sec'01), June 11-13, 2001, Paris, France. IFIP Conference Proceedings 193, ISBN 0-7923-7389-8, Kluwer, pp. 385-402, 2001.

[2] Chu-Hsing Lin; Chen-Yu Lee;. *One-time installation with traitors tracing for copyright programs.* Security Technology, 2001 IEEE 35th International Carnahan Conference on , Oct 2001 Page(s): 149 -155.

[3] Katherine M. Shelfer; J. Drew Procaccino; *Smart card evolution*. Communications of the ACM July 2002, Volume 45 Issue 7

[4] O.Goldreich, *Towards a theory of software protection*, Proc. 19th Ann. ACM Symp. On Theory of Computing, pp. 182-194. 1987